1. (Twice Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data; [and]

a medium personal number which is [unique for each storage medium] particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite[,]; and [said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer]

permission information which includes a decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer.

6. (Twice Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data; [and]

a medium personal number which is [unique for each storage medium] particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite[,]; and

[said medium personal number is used for generating an encrypted permission information in said vendor computer]

permission information encrypted in a manner that is generated independent from a specific apparatus number for a specific computer.

11. (Twice Amended) A storage medium accessed by a vendor computer and a user computer said storage medium for storing information readable by said user computer said storage medium comprising:

encrypted electronic data;

a medium personal number which is [unique for each storage medium] particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

encrypted permission information that is independent from a specific apparatus number for a specific computer;

wherein at least the medium personal number is written onto the storage medium in an unrewritable form which a user computer cannot rewrite.

17. (Twice Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

electronic information; and

information which is encrypted based on said medium personal number and independent from a specific apparatus number for a specific computer and said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer.

18. (Twice Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic information;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number is used for decrypting said encrypted electronic information; and information which is encrypted based on said medium personal number and independent from a specific apparatus number for a specific computer.

19. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and a third storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific first computer.

23. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the decryption key and which stores the encrypted electronic information onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the encrypted decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific first computer.

24. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from a specific apparatus number for a specific computer.

25. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the encrypted decryption key and which stores the encrypted electronic information onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from a specific apparatus number for a specific computer.

26. (Twice Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon a medium personal number and independent from a specific apparatus number for a specific computer, and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that

has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific computer.

27. (Twice Amended) A storage medium accessible from different computers at different times, the storage medium comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from a specific apparatus number for a specific computer.

28. (Twice Amended) A storage medium accessed by a computer, said storage medium, comprising:

a first storage area for storing encrypted electronic information, the encrypted electronic information includes electronic information encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is based upon the medium personal number and the decryption key is independent from a specific apparatus number for a specific computer.

29. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted

decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific first computer.

33. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the decryption key and which stores the encrypted electronic information onto the storage medium, and accessible from a plurality of second computers which decrypt the

encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific second computer.

34. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and a storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific computer.

35. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the decryption key and which stores the encrypted electronic information onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific computer.

36. (Twice Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which decrypt encrypted

electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from the specific apparatus number for the specific computer.

37. (Twice Amended) A storage medium accessible from different computers at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing an encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from a specific apparatus number for a specific computer.

38. (Twice Amended) A storage medium accessed by a computer, said storage medium, comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing an encrypted decryption key, wherein the decryption key is based upon the medium personal number and the encrypted decryption key is independent from a specific apparatus number for a specific computer.

39. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific first computer.

43. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the decryption key and which stores the encrypted electronic information onto the storage medium, and accessible from a plurality of second computers which the decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific second computer.

44. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

45. (Twice Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a

specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic information based upon the decryption key and which stores the encrypted electronic information onto the storage medium, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

46. (Twice Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which decrypt encrypted electronic information stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, comprising:

a storage area for storing the medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

47. (Twice Amended) A storage medium accessible from different computers at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from a specific apparatus number for a specific computer.

48. (Once Amended) A storage medium accessed by a computer, said storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from a specific apparatus number for a specific computer.

49. (Twice Amended) A storage medium accessed by a computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

53. (Twice Amended) A storage medium accessed by a computer in a manner such that a decryption key is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic information is encrypted based upon the decryption key and the encrypted electronic information is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular second computer in different time, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

54. (Twice Amended) A storage medium accessed by a computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and that the encrypted decryption key is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

55. (Twice Amended) A storage medium accessed by a computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic information is encrypted based upon the decryption key and the encrypted electronic information is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

56. (Twice Amended) A storage medium accessed by a computer in a manner such that an encrypted decryption key stored on the storage medium is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted information which includes information encrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer.

103. (Twice Amended) A method for a computer to access encrypted data on a storage medium, the method comprising:

obtaining first data based on a medium personal number and independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium;

decrypting the data based on the first data; and

accessing the decrypted data.

107. (Twice Amended) A method for a computer to provide encrypted data to a storage medium, the method comprising:

obtaining first data based on a medium personal number and independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium;

encrypting the data based on the first data; and

providing the encrypted data to the storage medium.

111. (Once Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot change; and

an area storing permission information which includes a decryption key encrypted in a manner that is independent from a specific apparatus number for a specific computer.

112. (Once Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot rewrite; and

an area storing permission information encrypted in a manner that is independent from a specific apparatus number for a specific computer.

113. (Twice Amended) A storage medium accessed by a vendor computer and a user computer said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

an area storing encrypted permission information that is independent from a specific apparatus number for a specific computer;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which a user computer cannot rewrite.

119. (Twice Amended) A storage medium readable by a computer, said storage medium comprising:

encrypted data; and

first data that is based on a medium personal number and independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the first data is used by the computer to decrypt the encrypted data.

123. (Twice Amended) A storage medium readable by different computers at different times, the storage medium comprising:

encrypted data; and

first data that is based on a medium personal number and independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the first data is used by the computer to decrypt the encrypted data.

124. (Once Amended) A storage medium for storing data for access and processing by a storage reading apparatus, said storage medium comprising:

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

an electronic information storage area including electronic information; and an information storage area including information which is encrypted based on said medium personal number and independent from a specific apparatus number for a specific computer.

125. (Once Amended) A storage medium for storing data for access and processing by a user storage reading apparatus, said storage medium comprising:

an encrypted electronic information storage area including encrypted electronic information;

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number is used for decrypting said encrypted electronic information; and

an information storage area including information which is encrypted based on said medium personal number and independent from a specific apparatus number for a specific computer.

REMARKS

As discussed during the telephone interview of May 8, 2002, the Official Action dated December 6, 2001 has been received and carefully noted. The period for response having been extended from March 6, 2002 to June 6, 2002 by the attached Petition for Extension of Time, the above amendments and the following remarks are submitted as a full and complete response thereto.

Claims 57-102 and 114-118 have been cancelled without prejudice. Claims 1-56, 103-113, and 119-125 have been amended to more particularly point out and distinctly claim the subject matter of the invention. These amendments are submitted to address the issues noted in the Official Action, to place the claims in compliance with reissue practice, and to place this application in condition for allowance. No new matter has been added, and no new issues are raised which require further consideration and/or search. These amendments are submitted to address the issues noted in the Official Action, and to correct the errors noted in the Reissue Declaration.

Claims 1-10 and 17-125, as submitted on October 2, 2001, were rejected under 35 USC § 251 as attempting to improperly recapture surrendered subject matter. Applicants respectfully submit that claims 1-56, 103-113, and 119-125 are in compliance with United States patent practice, and recite subject matter which should, in this reissue application, be allowed. The Office Action took the position, on the bottom of page 3, that claims 1, 6 and 17-25 did not include limitations regarding generation of the decryption key or encrypted permission information. The Official Action also took the position that claims 17-125 did not include limitations that provided a basis for imparting functionality from the storage medium to a computer. With respect to the generation of a decryption key or encrypted permission information, applicants respectfully submit that the claims, for example, claim 1, include a recitation of permission information which includes a decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer. Claims 6, 17-56, 103-113 and 119-125 recite similar aspects regarding the decryption key, encrypted permission information, and functionality regarding a computer.

Applicants further respectfully direct the Examiner's attention to claim 11 of issued United States Patent No. 5,796,824. MPEP § 1412.03 makes it clear that a claim in a reissue application is not considered to be broadened if the claim is narrower than, or equal in scope to, any other claim which appears in the patent. Patented claim 11 is directed to a storage medium accessed by a vendor computer and a user computer, with the storage medium for storing information readable by the user computer. The storage medium comprises encrypted electronic data, and a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium. Encrypted permission information is provided; at least the medium personal number is written onto the storage medium in an unrewritable form, which a user computer cannot rewrite. Although amendments have been made to the claims in order to correct the errors noted in the Reissue Declaration, it is respectfully submitted that the amendments to the claims and the subject matter presently pending in this application does not constitute an impermissible recapture under 35 USC § 251. Although the scope of the claims is not identical, it is respectfully submitted that the claims in their current form, and claim 11 as issued in Patent No. 5,796,824, are evidence that there is no attempt at impermissible recapture herein.

Regarding claims 1 and 6, the Office Action stated that the claim did not include limitations regarding generation of a decryption key or encrypted permission information. However, no such limitations existed in claim 6 in the issued patent. However, applicants have made their best efforts to clarify this issue as discussed above, and to meet the requirements set forth in the Official Action.

Claims 1-125 were rejected under 35 USC § 112, second paragraph, as being indefinite. The Official Action cited numerous deficiencies in these claims, and raised questions regarding adequate support for these amendments in the specification. In Paragraph 4 of the Official Action, the Office Action took the position that the limitation "that is not dependent on a specific device identifier for a specific device" is ambiguous since the storage medium is a specific device having a specific device identifier. The claims have been amended to more particularly point out and distinctly claim the specific device identifier as being a specific apparatus number, and the specific device is recited as being a specific computer. It is respectfully submitted that this aspect of the rejection has been overcome by the amendments made in the response.

In further detail, it appears that the Official Action has construed the meaning of the terms "specific identifier" and "medium personal number" to be interchangeable. As a preliminary matter, "specific identifier" has been changed to specific apparatus number, as discussed above. Additionally, "specific apparatus number" and "medium personal number" are separate and distinct aspects of the invention. Referring, for example, to column 5, lines 23-24 of the '824 patent, medium personal number 12 is a particular personal number for medium 11. Regarding "specific apparatus number", applicants point out that the Manual of Patent Examining Procedure permits an applicant to be his or own lexicographer. It is respectfully submitted that the term "specific apparatus number" has been discussed in the specification, for example, column 2, lines 40-41, 46, 56, 58, and 65. Additionally, the specification clearly discusses that the invention generates a medium number which is written on the storage medium in an un-rewritable form by the user's computer so that the permission information may be stored on another medium. According to the present invention, it is possible to transfer the stored data to another user so that the stored medium may be used in another computer. Therefore, the generation of permission information in the present invention, is not linked, associated, or limited to be used only with a specific computer having a specific computer identification number. In the context of the present invention, the storage medium may be used with any computer because the permission information does not rely upon the computers assigned identification or serial number. The storage medium of the present invention may be used with multiple computers without checking or verifying whether the storage medium is authorized to operate on a particular computer having a designated identification number. The storage medium may be used in another computer, regardless of the computer's specific identification number.

It is therefore respectfully requested that the rejection of claims 1-25 under 35 USC § 112, second paragraph, be withdrawn.

Claims 19-125 were also rejected under 35 USC § 112, second paragraph, as being indefinite. The Official Action took the position that the claims were indefinite and unclear regarding how they differentiate from each other. As noted above, claims 57-102 and 114-118 have been cancelled without prejudice. Remaining claims 1-56, 103-113 and 119-125 have all been submitted to address the deficiency noted in the Declaration, in that the claims as originally filed did not properly protect the applicants' invention. In particular, the patented claims did not include claims directed to a storage medium comprising a medium personal number and electronic information where the electronic information is encrypted based upon the medium personal number. The patented claims also were not directed to a storage medium which comprised encrypted electronic information and a medium personal number which is used for decrypting the encrypted electronic information which is based upon the medium personal number as described within the specification. It is respectfully submitted that the deletion of the claims noted above, as well as the amendments of the claims, make it clear that the claimed invention is directed to methods and apparatuses as described in the specification, and are claimed in such a way as to cure the deficiencies noted in the Reissue Declaration. Claims 19-22 are directed to a system wherein a storage medium is accessible from a first computer and a plurality of second computers. Claim 23 is similar to claim 19, but recites additional specificity in the preamble regarding encryption of electronic information based upon the decryption key, and which stores the encrypted electronic information onto the storage medium. Claim 24 is similar to claim 19, but does not include a limitation regarding being accessible from a plurality of second computers. Claim 25 is similar to claim 23, but also does not include the limitation regarding a plurality of second computers. Claim 26 is similar to claim 19, but does not include a limitation regarding a first computer and second computers. Claim 27 is similar to claim 19, but recites that the storage medium is accessible from different computers at different times. The preamble of claim 27, therefore, is much shorter than the preamble of claim 19. Claim 28 is similar to claim 19, but also does not include the information in the preamble. Claims 29-38 are similar to claims 19-28, but does not have reference to first storage area, second storage area, and third storage area. Claims 39-48 are similar to claims 29-38, but refers to storing of encrypted information which includes information encrypted based upon the medium personal number, rather than referring to decryption key.

Claims 49-56 are similar to claims 39-46, but the preambles are not directed to first computers and second computers. Claims 103-110 are directed to a method for a computer to access encrypted data, while the previously-discussed claims are directed to various storage mediums. Claims 111-113 are similar to claims 1, 6, and 11, but refer to particular storage areas rather than the encrypted electronic data, medium personal number, and permission information.

Claims 119-123 are directed to a storage medium readable by a computer, with the storage medium comprising encrypted data and first data. Claims 124 and 125 are also directed to a storage medium, with the storage medium for storing data for access and processing by a storage reading apparatus, with the storage medium comprising a medium personal number storage area, an electronic information storage area, and an information storage area. Claim 125 recites additional aspects of the medium personal number storage area.

Applicants respectfully submit, therefore, that the rejection of claims 1-125 (pending claims 1-56, 103-113, and 119-125) under 35 USC § 112, second paragraph, has been overcome.

Claims 1-125 were separately rejected under 35 USC § 112, first paragraph, as being directed to subject matter which was not described in the specification so as to reasonably convey to one skilled in the art that the inventors had possession of the claimed invention at the time that the invention was filed. As discussed above, applicants respectfully submit that the specific apparatus number, and the interrelationship of the specific apparatus number to the storage medium and to a specific computer, has been fully described and discussed in the specification, such as column 2, lines 40, 41, 46, 56, 58, and 65. The term "specific identifier" relates to a computer identification number such a serial number, and, therefore, the claims discuss decryption keys and other aspects which are generated independent from a specific apparatus number for a specific computer is such that the storage medium is not limited to be used with a specific computer assigned a specific apparatus number. It is respectfully submitted, therefore, that claims 1-125 are directed to subject matter which is, in fact, appropriately conveyed to a person of ordinary skill in the art.

Claims 1-125 were separately rejected under 35 USC § 112, first paragraph, as failing to enable a person of ordinary skill in the art to make and/or use the invention. Once again, applicants respectfully submit that the specification and claims are in compliance with United States patent practice. For example, in one embodiment of the invention, the permission key information is generated by the software decrypting key corresponding to the software to be sold, is taken from the software decrypting key management table 5. This key is input to encrypting circuit 231. The software decrypting key is encrypted by the personal key in the encrypting circuit 231. Encrypting circuit 231 generates the permission information 13. Permission information 13 includes the software name, having the escape character ENC and the encrypted information. Permission information 13 is stored on the software storage medium 11. The software decrypting key, and the algorithm or secret key are protected by a known encryption means. The vendor generates the medium key based on the medium number 12, read from the software storage medium 11. The vendor then encrypts the software decrypting key based on the medium key, and stores the software decrypted key into the software storage medium 11 as the permission information 13. See, for example, column 8, lines 3-15 of the specification.

The specification also discusses transfer of the permission information. One example explains that permission information 13 may be provided from the vendor directly to the user to permit the use of the software (column 5, lines 33-34). Another embodiment, discussed in column 4, lines 60-64, discusses that the vendor may transfer the permission information to the user's computer through a transmission line, so that the user's computer can decrypt the encrypted electronic data based on the permission information to provide the plain text electronic data. A further embodiment, discussed in column 4, lines 57-60, proposes that permission information may be stored on a floppy disk by the vendor and provided for use in the user's computer when the floppy disk is inserted into the disk drive of the computer.

In summary, applicants respectfully submit that the specification provides sufficient information to enable a person of ordinary skill in the art to make and use the invention, and to show that the inventors were in possession of the invention sufficiently enough to convey to one skilled in the art how the invention operates.

Claims 1-10, 17-94, and 124-125 were rejected under 35 USC § 101 as being directed to non-statutory subject matter. Applicants respectfully submit that a wealth of case law exists which enables applicant to draft claims directed to the machine, process, composition of matter, etc. or for any new and useful improvement thereof (see 35 USC § 101). Of course, court interpretations of this statute have placed various requirements on the claims, such that they be directed to a process which provides a useful, concrete, and tangible result, and which is not directed to computer programs or data structures per se.

Applicants respectfully submit, however, that the presently pending claims are directed to a storage medium (or methods) which contain specific information thereon, wherein this information is arranged in such a way so as to provide a useful, concrete, and tangible result. A storage medium is, per se, an article of manufacture. It is not, therefore, a computer program per se, or a mathematical algorithm. Additionally, the information on the storage medium, in claim 1 as an example, is recited as including a decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer. This is, therefore, one example of the useful, concrete, and tangible result which is currently required by United States patent practice.

Claims 1, 2, 6, 7, 11, 12, 17-20, 29, 30, 39, 40, 49, 50, 57, 58, 67, 68, 77, 78, 87, 88, and 91-125 were rejected under 35 USC § 102(b) as being anticipated by Matyas '534 (U.S. Patent No. 4,757,534). Applicants respectfully submit that each of claims 1-56, 103-113, and 119-125 recite subject matter which is neither disclosed nor suggested in Matyas.

As discussed above, and in applicants' previous responses, the present invention is directed to various embodiments of a storage medium, and methods, of handling and providing encrypted data on a storage medium. For example, claim 1 is directed to a storage medium accessed by a vendor computer and user computer. The storage medium stores information readable by the user computer, and comprises encrypted electronic data, and a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium. At least the medium personal number is written on to the storage medium in an un-rewritable form which the user computer cannot rewrite. Permission information is also provided, and includes a decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer.

As another example, claim 103 is directed to a method for a computer to access encrypted data on a storage medium. The method of claim 103 comprises obtaining first data based upon a medium personal number and independent from a specific apparatus number for a specific computer. The medium personal number is un-rewritable and particularly personal for each storage medium, and is different from a medium personal number of another storage medium. The method then comprises decrypting the data based on the first data, then accessing the decrypted data. In other words, the storage medium of the present invention, and the method according to the present invention, provides a secure storage medium which can, in fact, be read by multiple computers. Encrypted information is not bound to a specific computer, and provides, therefore, encrypted information on a medium that can be used on a variety of computers. It is respectfully submitted that the prior art of Matyas fails to disclose or suggest the claimed invention.

Matyas is directed to a storage medium that binds encrypted data to a specific computer so that "only the designated computer is capable of generating the decryption key that will produce the file key KF." In the response which applicants filed on July 19, 2001, these arguments were clearly and specifically set forth.

Additionally, Matyas is replete with statements that clarify that the method of Matyas is limited to operate only with a specific, designated computer. Referring for example to column 2, lines 32-38, 42, 43, 52, 53, as well as column 5, lines 12-22, column 6, lines 2-7, 38-40 and 52, and elsewhere, statements are clearly evident. The Official Action, however, seemed to take the position that Matyas discloses that a secret key may be assigned to a user, and not a specific computer, by way of a password. The Official Action referred to column 6, line 56 as supporting this proposition. However, it is respectfully submitted that the explanation in column 6, lines 59-66 of Matyas provides an explanation about how a password is generated. However, this single passage must be read in conjunction with the other teachings of Matyas. Column 5, line 62 - Column 8, line 16, and as illustrated in Figure 3, provide the explanation of how the password works in conjunction with the other aspects of Matyas. Matyas specifically discloses that in order to obtain the password, after purchasing the software, the purchaser or user must call the software vendor and supply the vendor with four types of information; the program number, the authorization number, the diskette serial number, and "the computer number." Column 6, lines 2-7 of Matyas state that "each computer 10 has a unique identification or number that is provided on the cover, for example, by a press-on label visible to the user." This identification or number is associated with the secret key of the crypto facility of the computer. If this is a first use of the software, Matyas verifies that the n-bit of the reference authorization number matches the authorization number provided by the caller. If so, Matyas then generates a password that will allow the encrypted program to be decrypted and executed <u>at the designated computer</u>. To produce the password, the key distribution center 14 encrypts the computer number with a key, KT, to produce an encryption key, KTTR, which is unique to that particular computer. (Matyas col. 6, lines 44- 47). Matyas further discusses in col. 6, lines 59 - 66 that based upon the program number provided by the caller the database of the software vendor produces a file key, KF. The key KF is then encrypted in the encryption block 34 (Fig. 3) with the cryptographic key KTTR returned by the key distribution center 14 to generate the password. As discussed above, the KTTR is the encryption key which is unique to the particular computer. After the key KF is encrypted with cryptographic key KTTR, then the generated password is then given to the caller. Thus, key KF, discussed in col. 6, lines 59-66, is encrypted with the KTTR so that key KF is limited and bound to operate with a designated computer. Further support for this proper interpretation of Matyas can be found in col. 8, lines 8 - 16, which further explains the encryption process. Matyas states, "The program number and diskette serial number concatenated together are encrypted in encryption block 103 with the encryption key for that particular computer to produce a decryption key which is used in decryption block 105 to decrypt the password and produce the secret file key, KF, that is used in decrypting the program or a portion of the program. . . Note that only the designated computer is capable of generating the decryption key that will produce the file key, KF." In addition, block 34 of Fig. 3 explicitly shows that key KF, which is transmitted from block 32, is encrypted by cryptographic key KTTR, which is transmitted from block 30. Therefore, applicants respectfully submit that Matyas is directed to a method that confines the content to a particular computer or apparatus. Therefore, the medium in Matyas is not portable; it can only be used with a single, particular apparatus, and cannot be used with multiple computers as can a storage medium of the present invention. Matyas, therefore, cannot be interpreted as disclosing or suggesting methods according to the present invention. Matyas, therefore, essentially discloses a conventional system as disclosed in Figure 1 of the present application. The present invention avoids the problems of the prior art, including Matyas, by not binding the encrypted information to a specific computer. As a result, the present invention provides encrypted information on a medium that can be easily used on a variety of computers. However, the encrypted information on a copied medium cannot be used on any computer. Without the original medium identifier, information cannot properly be decrypted. It is respectfully submitted, therefore, that Matyas is not a proper reference upon which to base a rejection of any of the presently pending claims.

Claims 3-5, 8-10, 13-16, 21, 22, 31, 32, 41, 42, 51, 52, 59, 60, 69, 70, 79, 80, 89, and 90 were rejected under 35 USC § 103(a) as being unpatentable over Matyas '534 in view of Shear (U.S. Patent No. 4,827,508). The Official Action took the position that Matyas '534 disclosed all of the elements of the claimed invention, with the exception of using an optical disk or a CD ROM, instead of the diskette of Matyas. However, applicants respectfully submit that Shear fails to cure the significant deficiencies which are discussed above.

The claims which are rejected based upon the combination of Matyas and Shear are primarily dependent claims, and include the limitations of the independent claims as discussed above. Shear is only directed to a database usage metering and protection system and method, and is cited purely for the disclosure therein of an optical disk or CD-ROM. However, a combination of Matyas and Shear fails to disclose or suggest a storage medium, or a method, which provides the critical and unobvious advantages discussed above, and which therefore contain the structure or steps of the claimed invention. A combination of Matyas and Shear would not disclose or suggest either a storage medium or a method wherein a medium personal number is written on to the storage medium in an un-rewritable form which a user storage reading apparatus or user computer cannot rewrite, in conjunction with electronic information, and information which is encrypted based on the medium personal number and not on a specific apparatus number for a specific computer. Therefore, the combination of Matyas and Shear would result in a diskette or other storage medium which is only readable on a single computer, while the present invention allows the encrypted information to be read by multiple computers.

In view of the above, applicants respectfully request that claims 1-56, 103-113, and 119-125 be found allowable, and this application passed to issue.

The present application and the above amendments were briefly discussed in a telephone interview between Examiner Gilberto Barron and applicants' representative on May 8, 2002. Applicants appreciate the Examiner's time and courtesy in conducting this telephone interview. During this telephone interview, applicants requested a personal interview to discuss this issue. The Examiner indicated that it would be preferable for applicants to file a written response, for the Examiner's consideration. It is respectfully submitted, therefore, that this written response is submitted, in an effort to expedite the allowance of this application. In the event that this application is not in fact found to be allowable, it is respectfully requested that the Examiner contact the undersigned attorney to arrange for an interview and discuss, if necessary, the filing of an appeal or a continuation application in order to continue the prosecution of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Douglas H. Goldhush
Registration No. 33,125

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DHG:scc
Enclosures: Petition for Extension of Time (3 months)
Notice of Appeal
Marked-up Copy of Amended Claims